GDPR e sistemi di pagamento digitali nei comuni: conformità e sicurezza

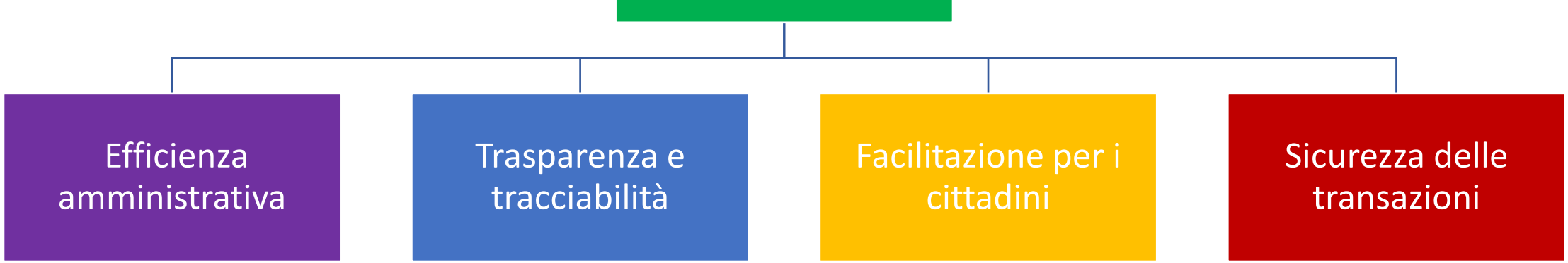
A domanda risponde Prof. Avv. Michele IASELLI

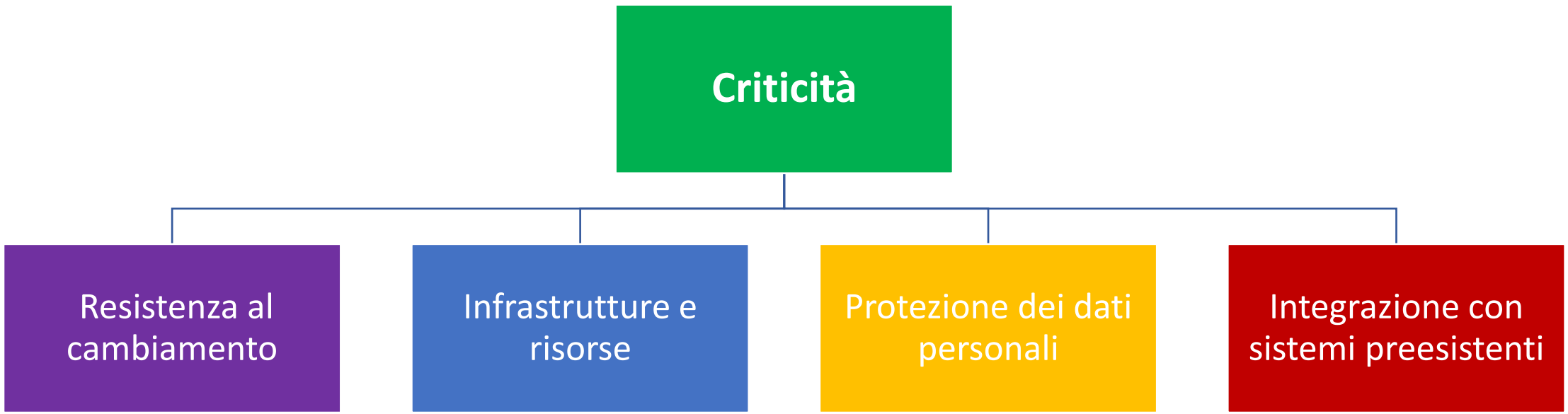
23 gennaio 2025 - dalle ore 11.30 alle 12.30

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione
degli Enti Locali
Email info@dpoinrete.it
Numero Verde 800.16.56.54
Web: www.dpoinrete.it
www.asmel.eu

La digitalizzazione dei pagamenti rappresenta uno degli elementi chiave per modernizzare i servizi pubblici e migliorare l'interazione tra cittadini, imprese e amministrazioni locali. Negli ultimi anni, le iniziative normative e strategiche hanno spinto i Comuni a implementare sistemi di pagamento digitale per agevolare la trasparenza, semplificare le procedure amministrative e migliorare l'efficienza della gestione pubblica.

Vantaggi e criticità


Vantaggi
Efficienza amministrativa
Trasparenza e tracciabilità
Facilitazione per i cittadini
Sicurezza delle transazioni


Criticità
Resistenza al cambiamento
Infrastrutture e risorse
Protezione dei dati personali
Integrazione con sistemi preesistenti

Principali strumenti utilizzati

dpo in rete

- PagoPA
- Portali comunali
- App per pagamenti
- Sistemi di e-commerce per la PA

Best practices per l’implementazione

dpo in rete

- Analisi preliminare
- Formazione e sensibilizzazione
- Collaborazione con partner tecnologici
- Monitoraggio continuo

Quadro normativo

dpo in rete

- Applicazione del GDPR
- Norme specifiche per i sistemi di pagamento
- Relazione tra GDPR ed altre normative
- Obblighi specifici per i Comuni
- Sanzioni e responsabilità
- Best practices per la conformità normativa

Raccolta e trattamento dei dati personali nei sistemi di pagamento

dpo in rete

- Tipologia dei dati personali raccolti e trattati
- Obblighi di informazione e trasparenza
- Base giuridica per il trattamento dei dati
- Gestione della minimizzazione dei dati
- Obblighi di sicurezza nel trattamento
- Gestione del ciclo di vita dei dati
- Best practices operative

Ruolo del titolare e del responsabile del trattamento nei sistemi di pagamento digitali

- Il Comune come titolare del trattamento
- Ruolo dei fornitori come responsabili del trattamento
- Clausole contrattuali tra titolare e responsabile
- Controlli ed audit sul responsabile del trattamento
- Differenze di responsabilità tra titolare e responsabile


Best practices
Mappatura dei ruoli
Contratti ben definiti
Valutazione periodica dei fornitori
Formazione interna
Supervisione continua

Misure di sicurezza per la protezione dei dati personali nei sistemi di pagamento

La sicurezza dei dati personali nei sistemi di pagamento digitali è una priorità assoluta per prevenire accessi non autorizzati, violazioni dei dati e frodi. Ai sensi dell'art. 32 del GDPR, i Comuni, in qualità di titolari del trattamento, e i fornitori di servizi di pagamento, come responsabili, devono implementare misure tecniche e organizzative adeguate al rischio.

- Misure tecniche per la protezione dei dati
- Misure organizzative
- Sicurezza delle transazioni
- Prevenzione e gestione dei data breach
- Misure avanzate per la sicurezza dei sistemi
- Controllo e audit

Best practices

Azione	Descrizione
Crittografia end-to-end	Protezione dei dati dall'origine alla destinazione.
Backup regolari e testati	Copie sicure dei dati conservate in luoghi separati.
Segmentazione della rete	Separare i sistemi critici per limitare l'impatto di un attacco.
Monitoraggio 24/7	Sorveglianza continua delle infrastrutture per rilevare anomalie.
Penetration testing	Simulazione di attacchi per identificare vulnerabilità prima che vengano sfruttate.

Conservazione e cancellazione dei dati nei sistemi di pagamento

La gestione dei dati personali nei sistemi di pagamento digitali deve rispettare il principio di limitazione della conservazione stabilito dall'Articolo 5, par. 1, lett.e) del GDPR. Questo principio impone che i dati personali siano conservati solo per il tempo strettamente necessario a soddisfare le finalità del trattamento.

- Definizione delle politiche di conservazione
- Cancellazione ed anonimizzazione dei dati
- Obblighi relativi a conservazione e cancellazione
- Gestione delle richieste degli interessati
- Politiche di sicurezza per la cancellazione

Best practices

Azione	Descrizione
Definire una retention policy	Redigere e pubblicare un documento che stabilisca i tempi di conservazione per ogni categoria di dati.
Automatizzare la cancellazione	Utilizzare software per la rimozione automatica dei dati al termine del periodo di conservazione.
Gestione integrata dei backup	Sincronizzare le politiche di cancellazione con i sistemi di backup per evitare incongruenze.
Formazione del personale	Addestrare gli operatori sull'importanza della gestione del ciclo di vita dei dati.